AF IFW

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 10016933-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): George S. GALES et al.

Confirmation No.: 2381

Application No.: 10/001,431

Examiner: Perungavoor, Venkatanaray

Filing Date: October 31, 2001

Group Art Unit: 2132

Title: SYSTEM AND METHOD OF DEFINING THE SECURITY CONDITION OF A COMPUTER SYSTEM

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on October 25, 2005.

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) $500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

☐ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

☐ 1st Month $120	☐ 2nd Month $450	☐ 3rd Month $1020	☐ 4th Month $1590

☐ The extension fee has already been filed in this application.

☒ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of $ 500. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees. A duplicate copy of this sheet is enclosed.

☒ I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:
Commissioner for Patents, Alexandria, VA 22313-1450
Date of Deposit: December 20, 2005

OR

☐ I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (571)273-8300.
Date of facsimile:
Typed Name: Cindy C. Dioso
Signature: Cindy C. Dioso

Respectfully submitted,

George S. GALES et al.

By James L. Baudino

James L. Baudino

Attorney/Agent for Applicant(s)

Reg No. : 43,486

Date : December 20, 2005

Telephone : (214) 855-7544

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPEAL FROM THE EXAMINER TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:	George S. GALES et al.	Confirmation No. 2381
Serial No.:	10/001,431	
Filing Date:	October 31, 2001	
Group Art Unit:	2132	
Examiner:	Perungavoor, Venkatanaray	
Title:	SYSTEM AND METHOD OF DEFINING THE SECURITY CONDITION OF A COMPUTER SYSTEM	
Docket No.:	10016933-1	

MAIL STOP: APPEAL BRIEF PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Sir:

APPEAL BRIEF

Applicants has appealed to the Board of Patent Appeals and Interferences from the decision of the Examiner mailed August 13, 2005, finally rejecting Claims 1-29. Applicants filed a Notice of Appeal on October 25, 2005. Applicants respectfully submits herewith this Appeal Brief with authorization to charge the statutory fee of $500.00.

12/28/2005 CCHAU1 00000019 082025 10001431
01 FC:1402 500.00 DA

REAL PARTY IN INTEREST

The present application was assigned to Hewlett-Packard Company as indicated by an assignment from the inventor recorded on March 13, 2002 in the Assignment Records of the United States Patent and Trademark Office at Reel 012736, Frame 0297. The present application was subsequently assigned to Hewlett-Packard Development Company, L.P. as indicated by an assignment from Hewlett-Packard Company recorded on September 30, 2003 in the Assignment Records of the United States Patent and Trademark Office at Reel 014061, Frame 0492.

RELATED APPEALS AND INTERFERENCES

There are no known appeals or interferences that will directly affect or be directly affected by or have a bearing on the Board's decision in this pending appeal.

STATUS OF CLAIMS

Claims 1-29 stand rejected pursuant to a Final Office Action mailed August 31, 2005. Claims 1-29 are presented for appeal.

STATUS OF AMENDMENTS

No amendment has been filed subsequent to the mailing of the Final Office Action.

SUMMARY OF CLAIMED SUBJECT MATTER

Embodiments of the present invention as defined by independent Claim 1 are directed toward a method of defining the security condition of a computer system (30, 60, 61, 62, 70, 71, 72, 73, 80, 81) comprising generating a human-readable and machine-readable vulnerability description language (VDL) file (200) specifying: an identity of an attack; at least one attribute of the specified attack; at least one policy definition with respect to the specified attack; and at least one attribute of the specified policy definition. (at least at page 7, lines 1-30; page 8, lines 11-45; page 9, lines 1-32; page 10, lines 1-31;

page 11, lines 7-17; page 21, line 23 to page 22, line 3; page 22, lines 26-30; and figures 2-4).

Embodiments of the present invention as defined by independent Claim 12 are directed toward a method of defining vulnerability conditions of a system (30, 60, 61, 62, 70, 71, 72, 73, 80, 81) coupled to a global network (50, 55, 56, 100, 212) comprising generating a human-readable and machine-readable vulnerability description language (VDL) file (200) specifying: a name of an attack associated with a vulnerability of the system (30, 60, 61, 62, 70, 71, 72, 73, 80, 81); at least one attribute of the specified attack, and the severity of the specified attack associated with a breach of the computer system (30, 60, 61, 62, 70, 71, 72, 73, 80, 81) by the specified attack; a policy definition with respect to the specified attack; at least one attribute of the specified policy definition; and a computing platform of the system (30, 60, 61, 62, 70, 71, 72, 73, 80, 81). (at least at page 7, lines 1-30; page 8, lines 11-45; page 9, lines 1-32; page 10, lines 1-31; page 11, lines 7-17; page 21, line 23 to page 22, line 3; page 22, lines 26-30; and figures 2-4).

Embodiments of the present invention as defined by independent Claim 17 are directed toward a system of defining security conditions of a computer system (30, 60, 61, 62, 70, 71, 72, 73, 80, 81) comprising: a human-readable and machine-readable vulnerability description language (VDL) file (200) containing a definition of at least one attack and a definition of at least one policy item for the attack, an interpreter (202) operable to parse the at least one attack and at least one policy item definition in the VDL file (200) and organize the parsed definitions pursuant to a predetermined format, and a data storage (204) operable to store the parsed and organized at least one attack and at least one policy item definition, wherein the data storage (204) is accessible by at least one security application (207, 208). (at least at page 7, lines 1-30; page 8, lines 11-45; page 9, lines 1-32; page 10, lines 1-31; page 11, lines 7-17; page 21, line 23 to page 22, line 3; page 22, lines 26-30; and figures 2-4).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1 and 3-29 are rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Publication No. 2002/011639 issued to Chefalas et al. (hereinafter "*Chefalas*").

2. Claim 2 is rejected under 35 U.S.C. §103(a) as being unpatentable over *Chefalas* in view of U.S. Patent No. 6,279,113 to Vaidya (hereinafter "*Vaidya*").

ARGUMENT

A. Standard

1. 35 U.S.C. § 102

Under 35 U.S.C. § 102, a claim is anticipated only if each and every element as set forth in the claim is found in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. of California*, 2 U.S.P.Q.2d 1051 (Fed. Cir. 1987); M.P.E.P. § 2131. In addition, "[t]he identical invention must be shown in as complete detail as is contained in the . . . claims" and "[t]he elements must be arranged as required by the claim." *Richardson v. Suzuki Motor Co.*, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989); *In re Bond*, 15 U.S.P.Q.2d 1566 (Fed. Cir. 1990); M.P.E.P. § 2131.

2. 35 U.S.C. § 103

To establish a *prima facie* case of obviousness under 35 U.S.C. § 103, three basic criteria must be met: First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings; second, there must be a reasonable expectation of success; and finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *In re Vaeck*, 947 F.2d 488, (Fed. Cir. 1991); M.P.E.P. § 2143. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. *Id.* Further, the mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680 (Fed.

Cir. 1990); M.P.E.P. § 2143.01. Additionally, not only must there be a suggestion to combine the functional or operational aspects of the combined references, but also the prior art is required to suggest both the combination of elements and the structure resulting from the combination. *Stiftung v. Renishw PLC*, 945 F.2d 1173, 1183 (Fed. Cir. 1991). Moreover, where there is no apparent disadvantage present in a particular prior art reference, then generally there can be no motivation to combine the teaching of another reference with the particular prior art reference. *Winner Int'l Royalty Corp. v. Wang*, 202 F.3d 1340, 1349 (Fed. Cir. 2000).

B. Argument

1. Claims 1-11

Claims 1 and 3-11 are rejected under 35 U.S.C. §102(e) as being anticipated by *Chefalas*. Claim 2 is rejected under 35 U.S.C. §103(a) as being unpatentable over *Chefalas* in view of *Vaidya*. Of the rejected claims, Claim 1 is independent. Applicants respectfully submit that independent Claim 1 is patentable over *Chefalas*. Therefore, independent Claim 1, and Claims 2-11 that depend therefrom, are allowable.

Embodiments of the present invention are directed generally toward a system and method for defining the security condition of a computer system (at least at page 8, lines 11-45; page 9, lines 1-32; page 10, lines 1-31; page 11, lines 7-17; page 21, line 23 to page 22, line 3; page 22, lines 26-30; and figures 2-4). For example, in some embodiments of the present invention, a human-readable and machine-readable vulnerability description language (VDL) file (200) is used to specify security and/or vulnerability descriptions of one or more computer systems as a collection of hierarchical security specifications (e.g., defined by product, category, and group definitions) (at least at page 8, lines 11-45; page 9, lines 1-32; page 10, lines 1-31; page 11, lines 7-17; page 21, line 23 to page 22, line 3; page 22, lines 26-30; and figures 2-4). In some embodiments of the present invention, the VDL file (200) describes the vulnerability of a computer system, how to test for its presence, how to report the detection of a vulnerability, and how to repair the vulnerability (at least at page 9, lines 1 to page 10,

line 31). The VDL file (200) is readable by humans as well as computer programs because of its syntax and format (at least at page 11, line 7 to page 21, line 16). The VDL file (200) is read and parsed to organize the vulnerability information into a form that can be accessed and used by security applications such as vulnerability scanners, intrusion detection systems and intrusion protection systems (at least at page 21, line 17 to page 22, line 2). Accordingly, for example, Claim 1 recites "generating a human-readable and machine-readable vulnerability description language (VDL) file specifying: an identity of an attack; at least one attribute of the specified attack; at least one policy definition with respect to the specified attack; and at least one attribute of the specified policy definition."

In the Final Office Action, the Examiner states that *Chefalas* discloses the limitations of independent Claim 1 (Final Office action, page 2). We disagree. *Chefalas* appears to disclose a set of software components that remove viruses from a computer system (e.g., a virus scanner controller (VSC) and a virus scanner and notifier (VSN)) (*Chefalas*, page 2, paragraph 0025). *Chefalas* also appears to disclose that in response to detecting a virus at a client computer, a server sends a business event to a remote administration system (*Chefalas*, page 5, paragraph 0054). *Chefalas* appears to disclose that the business event takes the form of a data packet which contains a header and a payload (*Chefalas*, page 4, paragraphs 0044 and 0045, figures 4A and 4B). *Chefalas* appears to disclose that the payload of the data packet may contain a virus name, action taken, and the computer ID (*Chefalas*, page 4, paragraphs 0044 and 0045, figures 4A and 4B). *Chefalas* further appears to disclose examples of rules, illustrated in a table, that may be used to implement business decisions as to how to handle the notification of the presence of a virus (e.g., different actions based on the name of the virus such as logging the action, scheduling maintenance, or paging a manager) (*Chefalas*, page 4, paragraphs 0046 and 0047, figures 5A and 5B). However, *Chefalas* does not disclose or even suggest that the rules illustrated in the tables of figures 5A and 5B of *Chefalas* are a "human-readable and machine-readable vulnerability description language (VDL) file" as recited by Claim 1 (emphasis added). To the contrary, figures 5A and 5B of *Chefalas*

appear to be nothing more than an illustration of policies presumably for the benefit of reader understanding of the *Chefalas* reference. *Chefalas* does not disclose or even suggest that such policies are in a file that is both human-readable and machine-readable because *Chefalas* is silent as to such. Therefore, for at least this reason, Applicants respectfully submit that *Chefalas* does not anticipate Claim 1.

Further, even if the rules illustrated in figures 5A and 5B of *Chefalas* were considered to be a human-readable and machine-readable vulnerability description language (VDL) file, which Applicants submit is not the case, Claim 1 recites that the VDL file specifies "an identity of an attack," "at least one attribute of the specified attack," "at least one policy definition with respect to the specified attack" and "at least one attribute of the specified policy definition." The rules illustrated in figure 5A of *Chefalas* appear to illustrate nothing more than a name of a virus and an action to be taken, and the rules illustrated in figure 5B of *Chefalas* appear to illustrate nothing more than a computer ID and an action to be taken. Thus, at the very least, *Chefalas* does not appear to disclose or even suggest a human-readable and machine-readable vulnerability description language (VDL) file specifying "at least one attribute of the specified attack" as recited by Claim 1. Therefore, for at least this reason also, Applicants respectfully submit that *Chefalas* does not anticipate Claim 1.

Accordingly, for at least the reasons discussed above, independent Claim 1 is clearly patentable over *Chefalas*. Moreover, *Vaidya* does not appear to remedy at least the deficiencies of *Chefalas* discussed above, nor did the Examiner rely on *Vaidya* to purportedly disclose any such deficiencies. Therefore, Claim 1, and Claims 2-11 that depend therefrom, are in condition for allowance.

2. Claims 12-16

Claims 12-16 are rejected under 35 U.S.C. §102(e) as being anticipated by *Chefalas*. Of the rejected claims, Claim 12 is independent. Applicants respectfully

submit that independent Claim 12 is patentable over *Chefalas*. Therefore, independent Claim 12, and Claims 13-16 that depend therefrom, are allowable.

Independent Claim 12 recites "generating a human-readable and machine-readable vulnerability description language (VDL) file specifying: a name of an attack associated with a vulnerability of the system; at least one attribute of the specified attack, and the severity of the specified attack associated with a breach of the computer system by the specified attack; a policy definition with respect to the specified attack; at least one attribute of the specified policy definition; and a computing platform of the system" (emphasis added). As discussed above in connection with independent Claim 1, *Chefalas* appears to disclose a set of software components that remove viruses from a computer system (e.g., a virus scanner controller (VSC) and a virus scanner and notifier (VSN)) (*Chefalas*, page 2, paragraph 0025). *Chefalas* also appears to disclose that in response to detecting a virus at a client computer, a server sends a business event to a remote administration system (*Chefalas*, page 5, paragraph 0054). *Chefalas* appears to disclose that the business event takes the form of a data packet which contains a header and a payload (*Chefalas*, page 4, paragraphs 0044 and 0045, figures 4A and 4B). *Chefalas* appears to disclose that the payload of the data packet may contain a virus name, action taken, and the computer ID (*Chefalas*, page 4, paragraphs 0044 and 0045, figures 4A and 4B). *Chefalas* further appears to disclose examples of rules, illustrated in a table, that may be used to implement business decisions as to how to handle the notification of the presence of a virus (e.g., different actions based on the name of the virus such as logging the action, scheduling maintenance, or paging a manager) (*Chefalas*, page 4, paragraphs 0046 and 0047, figures 5A and 5B). However, *Chefalas* does not disclose or even suggest that the rules illustrated in the tables of figures 5A and 5B of *Chefalas* are a "human-readable and machine-readable vulnerability description language (VDL) file" as recited by Claim 12. To the contrary, figures 5A and 5B of *Chefalas* appear to be nothing more than an illustration of policies presumably for the benefit of reader understanding of the *Chefalas* reference. *Chefalas* does not disclose or even suggest that such policies are in a file that is both human-readable and machine-readable because

Chefalas is silent as to such. Therefore, for at least this reason, Applicants respectfully submit that *Chefalas* does not anticipate Claim 12.

Further, even if the rules illustrated in figures 5A and 5B of *Chefalas* were considered to be a human-readable and machine-readable vulnerability description language (VDL) file, which Applicants submit is not the case, Claim 12 recites that the VDL file specifies "a name of an attack associated with a vulnerability of the system; at least one attribute of the specified attack, and the severity of the specified attack associated with a breach of the computer system by the specified attack; a policy definition with respect to the specified attack; at least one attribute of the specified policy definition; and a computing platform of the system" (emphasis added). The rules illustrated in figure 5A of *Chefalas* appear to illustrate nothing more than a name of a virus and an action to be taken, and the rules illustrated in figure 5B of *Chefalas* appear to illustrate nothing more than a computer ID and an action to be taken. Thus, at the very least, *Chefalas* does not appear to disclose or even suggest a human-readable and machine-readable vulnerability description language (VDL) file specifying "at least one attribute of the specified attack," a "severity of the specified attack" or "a computing platform of the system" as recited by Claim 12. Therefore, for at least these reasons also, Applicants respectfully submit that *Chefalas* does not anticipate Claim 12.

Accordingly, for at least the reasons discussed above, independent Claim 12 is clearly patentable over *Chefalas*. Therefore, Claim 12, and Claims 13-16 that depend therefrom, are in condition for allowance.

3. Claims 17-29

Claims 17-29 are rejected under 35 U.S.C. §102(e) as being anticipated by *Chefalas*. Of the rejected claims, Claim 17 is independent. Applicants respectfully submit that independent Claim 17 is patentable over *Chefalas*. Therefore, independent Claim 17, and Claims 18-29 that depend therefrom, are allowable.

Independent Claim 17 recites "a human-readable and machine-readable vulnerability description language (VDL) file containing a definition of at least one attack and a definition of at least one policy item for the attack," "an interpreter operable to parse the at least one attack and at least one policy item definition in the VDL file and organize the parsed definitions pursuant to a predetermined format" and "a data storage operable to store the parsed and organized at least one attack and at least one policy item definition, wherein the data storage is accessible by at least one security application" (emphasis added). As discussed above in connection with independent Claim 1, *Chefalas* appears to disclose a set of software components that remove viruses from a computer system (e.g., a virus scanner controller (VSC) and a virus scanner and notifier (VSN)) (*Chefalas*, page 2, paragraph 0025). *Chefalas* also appears to disclose that in response to detecting a virus at a client computer, a server sends a business event to a remote administration system (*Chefalas*, page 5, paragraph 0054). *Chefalas* appears to disclose that the business event takes the form of a data packet which contains a header and a payload (*Chefalas*, page 4, paragraphs 0044 and 0045, figures 4A and 4B). *Chefalas* appears to disclose that the payload of the data packet may contain a virus name, action taken, and the computer ID (*Chefalas*, page 4, paragraphs 0044 and 0045, figures 4A and 4B). *Chefalas* further appears to disclose examples of rules, illustrated in a table, that may be used to implement business decisions as to how to handle the notification of the presence of a virus (e.g., different actions based on the name of the virus such as logging the action, scheduling maintenance, or paging a manager) (*Chefalas*, page 4, paragraphs 0046 and 0047, figures 5A and 5B). However, *Chefalas* does not disclose or even suggest that the rules illustrated in the tables of figures 5A and 5B of *Chefalas* are a "human-readable and machine-readable vulnerability description language (VDL) file" as recited by Claim 17. To the contrary, figures 5A and 5B of *Chefalas* appear to be nothing more than an illustration of policies presumably for the benefit of reader understanding of the *Chefalas* reference. *Chefalas* does not disclose or even suggest that such policies are in a file that is both human-readable and machine-readable because *Chefalas* is silent as to such. Therefore, for at least this reason, Applicants respectfully submit that *Chefalas* does not anticipate Claim 17.

Further, independent Claim 17 recites "an interpreter operable to parse the at least one attack and at least one policy item definition in the VDL file and organize the parsed definitions pursuant to a predetermined format." In the Final office Action, the Examiner refers generally to figure 4A of *Chefalas* (which appears to illustrate a data packet) and paragraphs 0046-0048 of *Chefalas* (which appear to discuss the rules illustrated in figures 5A and 5B of *Chefalas*) (Final Office Action, pages 4 and 5). Applicants respectfully submit that *Chefalas* does not appear to disclose or even suggest, either in the portions of *Chefalas* referred to by the Examiner or elsewhere in *Chefalas*, "an interpreter operable to parse the at least one attack and at least one policy item definition in the VDL file and organize the parsed definitions pursuant to a predetermined format" as recited by Claim 17. In fact, the Examiner fails to explicitly identify what element or device of the *Chefalas* system the Examiner considers to correspond to the "interpreter" recited by Claim 17, thereby leaving Applicants to "guess" as to the basis of the Examiner's rejection of Claim 17, which is improper. Accordingly, for at least this reason also, Applicants respectfully submit that *Chefalas* does not anticipate Claim 17.

Additionally, Claim 17 recites "an interpreter operable to parse the at least one attack and at least one policy item definition in the VDL file and organize the parsed definitions pursuant to a predetermined format." In the Final Office Action, the Examiner appears to consider the rules illustrated in figures 5A and 5B of *Chefalas* as the "human-readable and machine-readable vulnerability description language (VDL) file" as recited by Claim 17 (Final Office Action, pages 2, 4 and 5). However, Claim 17 recites that the DVL file is parsed and organized "pursuant to a predetermined format." Thus, if the tables illustrated in figures 5A and 5B of *Chefalas* represent the "predetermined format" of information, the Examiner has not indicated or in any way identified the VDL file that is parsed and organized to arrive at the such information. Accordingly, for at least this reason also, Applicants respectfully submit that *Chefalas* does not anticipate Claim 17.

Accordingly, for at least the reasons discussed above, independent Claim 17 is clearly patentable over *Chefalas*. Therefore, Claim 17, and Claims 18-29 that depend therefrom, are in condition for allowance.

CONCLUSION

Applicants have demonstrated that the present invention as claimed is clearly distinguishable over the art cited of record. Therefore, Applicants respectfully request the Board of Patent Appeals and Interferences to reverse the final rejection of the Examiner and instruct the Examiner to issue a notice of allowance of all claims.

The Commissioner is authorized to charge the statutory fee of $500.00 to Deposit Account No. 08-2025 of Hewlett-Packard Company. Although no other fee is believed due, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 08-2025 of Hewlett-Packard Company.

Respectfully submitted,

James L. Baudino
Registration No. 43,486

Date: December 20, 2005

Correspondence To:

L. Joy Griebenow
Hewlett-Packard Company
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400
Tel. (970) 898-3884

CLAIMS APPENDIX

1. A method of defining the security condition of a computer system, comprising:

generating a human-readable and machine-readable vulnerability description language (VDL) file specifying:

an identity of an attack;

at least one attribute of the specified attack;

at least one policy definition with respect to the specified attack; and

at least one attribute of the specified policy definition.

2. The method, as set forth in claim 1, further comprising generating the VDL file specifying:

a computing platform of the computer system; and

a data signature of the specified attack on the computing platform.

3. The method, as set forth in claim 1, further comprising generating the VDL file specifying:

a security category of the specified attack; and

at least one policy group with respect to the specified security category.

4. The method, as set forth in claim 1, further comprising generating the VDL file specifying a security product executing on the computer system.

5. The method, as set forth in claim 1, wherein specifying at least one attribute of the specified attack comprises specifying an identification of the severity associated with a breach of the computer system by the specified attack.

6. The method, as set forth in claim 1, wherein specifying at least one attribute of the specified attack comprises specifying a description of the attack.

7. The method, as set forth in claim 1, wherein specifying at least one attribute of the specified attack comprises specifying an explanation of why the specified attack is important.

8. The method, as set forth in claim 1, wherein specifying at least one attribute of the specified attack comprises specifying how information is to be reported to a user with respect to the specified attack.

9. The method, as set forth in claim 1, wherein specifying at least one attribute of the specified attack comprises specifying an application operable to respond to a breach of the computer system by the specified attack.

10. The method, as set forth in claim 1, wherein specifying a signature of the specified attack comprises:

specifying a network protocol; specifying a data pattern; and

specifying an action in response to detecting the specified network protocol and data pattern.

11. The method, as set forth in claim 1, wherein specifying a signature of the specified attack comprises specifying a direction of data flow.

12. A method of defining vulnerability conditions of a system coupled to a global network, comprising:

generating a human-readable and machine-readable vulnerability description language (VDL) file specifying:

a name of an attack associated with a vulnerability of the system;

at least one attribute of the specified attack, and the severity of the specified attack associated with a breach of the computer system by the specified attack;

a policy definition with respect to the specified attack;

at least one attribute of the specified policy definition; and

a computing platform of the system.

13. The method, as set forth in claim 12, further comprising generating the VDL file specifying:

a security category of the specified attack; and

at least one policy group with respect to the specified security category.

14. The method, as set forth in claim 12, wherein specifying at least one attribute of the specified attack comprises specifying how information is to be reported to a user with respect to the specified attack.

15. The method, as set forth in claim 12, wherein specifying at least one attribute of the specified attack comprises specifying an application operable to respond to a breach of the computer system by the specified attack.

16. The method, as set forth in claim 12, wherein specifying at least one attribute of the specified attack comprises specifying a source of an application operable to repair the vulnerability.

17. A system of defining security conditions of a computer system, comprising:

a human-readable and machine-readable vulnerability description language (VDL) file containing a definition of at least one attack and a definition of at least one policy item for the attack;

an interpreter operable to parse the at least one attack and at least one policy item definition in the VDL file and organize the parsed definitions pursuant to a predetermined format; and

a data storage operable to store the parsed and organized at least one attack and at least one policy item definition, wherein the data storage is accessible by at least one security application.

18. The system, as set forth in claim 17, wherein the data storage is a relational database having a plurality of tables.

19. The system, as set forth in claim 17, wherein the data storage is a memory.

20. The system, as set forth in claim 17, wherein the VDL file further comprises a definition of a security product.

21. The system, as set forth in claim 17, wherein the VDL file further comprises a definition of a security category providing a grouping of the at least one attack, and a definition of a policy group providing a grouping of the at least one policy item.

22. The system, as set forth in claim 17, wherein the VDL file further comprises a definition of a computing platform.

23. The system, as set forth in claim 17, wherein the VDL file further comprises a definition of at least one attribute of the at least one attack.

24. The system, as set forth in claim 17, wherein the VDL file further comprises an identification of the severity associated with a breach of the computer system by the at least one attack.

25. The system, as set forth in claim 17, wherein the VDL file further comprises a description of the at least one attack.

26. The system, as set forth in claim 17, wherein the VDL file further comprises a definition of how information are to be displayed and reported to the user in response to generated results with respect to the at least one attack.

27. The system, as set forth in claim 17, wherein the VDL file further comprises a definition of an application operable to respond to a breach of the computer system by the at least one attack.

28. The system, as set forth in claim 17, wherein the VDL file further comprises a signature of the specified attack having:

a network protocol;

a data pattern; and

an action in response to detecting the specified network protocol and data pattern.

29. The system, as set forth in claim 17, wherein the VDL file further comprises a signature of the specified attack having a direction of data flow.

EVIDENCE APPENDIX

None

RELATED PROCEEDINGS APPENDIX

None